

REMARKS

Summary of Claim Status

Claims 1-29 are pending in the present application. Claims 1-21 and 29 are rejected for the reasons discussed below. Claims 22-28 are allowed. Applicants thank the Examiner for this acknowledgement of patentable subject matter.

Applicants respectfully request favorable reconsideration of the claims and withdrawal of the pending rejections in light of the following discussion.

Rejections Under 35 U.S.C. § 102

Claim 20 is rejected under 35 U.S.C. § 102(a) as being anticipated by Erickson, U.S. Patent No. 5,970,142 ("Erickson"). With respect to Claim 20, the Examiner stated:

Erickson discloses a PLD (column 1 line 63), which is inherently non-volatile, that receives an encrypted configuration bit stream (column 1 line 66 - column 2 line 1), including a key (column 1 lines 63), a decryptor that decrypts a part of the bit stream using the key (column 2 lines 1-3), and configures elements with the configuration data from the bit stream (column 2 lines 4-5).

(Office Action at page 2, ¶ 4.) Applicants respectfully traverse this rejection.

Applicants respectfully submit that the programmable logic device (PLD) disclosed in Erickson is not inherently non-volatile. As is well-known in the art, while some PLDs may be non-volatile, not all PLDs are non-volatile, and in fact many PLDs are volatile devices. Therefore, PLDs in general are not inherently non-volatile.

Furthermore, the disclosure of Erickson clearly contemplates a volatile PLD in at least some embodiments. For instance, Fig. 1 of Erickson shows a programmable logic device 110 and a storage device 120. As noted in Erickson, at power on, after certain initialization steps, storage device 120 transmits configuration data 135 to PLD 110. (See, e.g., Erickson at col. 3, lines 23-37.) This implies that PLD 110 does not retain configuration data when power is removed, and

instead relies on storage device 120 to provide the data at power on. Erickson lists some embodiments of storage device 120 such as EPROM, EEPROM, or ROM that are non-volatile embodiments for storing such data. (See, e.g., Erickson at col. 4, lines 32-40.) Therefore, Erickson does not disclose a PLD that is inherently non-volatile since in at least some of the embodiments contemplated by Erickson the PLD is clearly volatile.

Moreover, Erickson does not teach or even suggest a PLD that comprises non-volatile storage that stores a first key, as recited in Claim 20. In fact, Erickson teaches away from such a limitation. As disclosed in Fig. 3 of Erickson and the related text, key flip-flops 224 form a shift register for storing the key 180 in decryption circuit 115 of PLD 110. As is well-known, a flip-flop is a volatile storage element and does not retain data after power is removed. Thus, the embodiment shown in Erickson teaches storing a key in volatile storage, and not in non-volatile storage as recited in Claim 20.

Therefore, the PLD of Erickson is not inherently non-volatile, and in fact, Erickson teaches volatile storage for storing a key. Applicants submit that for at least these reasons, Erickson does not teach or suggest all the limitations of Claim 20. Applicants respectfully submit Claim 20 is patentable over the cited art, and request allowance of Claim 20.

Claim 21 depends from Claim 20, and thus includes all the limitations of Claim 20. Therefore, for at least the reasons set forth above with respect to Claim 20, Applicants believe Claim 21 is allowable and respectfully request its allowance.

Rejections Under 35 U.S.C. § 103

Claims 1-9 and 11-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson. With respect to Claim 1, the Office Action stated:

Erickson discloses a method of configuring a PLD with an encrypted bit stream . . . Erickson does not disclose using a unique private key to decrypt an

encrypted key to decrypt the bit stream, but mentions generating a key. The examiner takes official notice that public/private key encryption is often used to transmit session keys. It would have been obvious for one of ordinary skill in the art to send an encrypted key to the PLD, rather than have the PLD create it's own key, so each PLD wouldn't need to have it's own random number generator, thus lowering costs, which Erickson teaches to be desirable (column 7 lines 42-43).

(Office Action at page 3, ¶ 6.) Applicants respectfully traverse this rejection.

Independent Claim 1

As set forth above with respect to Claim 20, Erickson clearly contemplates embodiments in which the PLD is volatile, and teaches embodiments where a key is stored in a volatile storage. In contrast, Claim 1 recites "maintaining a device identifier and a private key in a programmable logic device, the device identifier and the private key being non-volatile such that if power to the programmable logic device is lost the device identifier and private key remain stored in the programmable logic device." As noted above, Erickson discloses an embodiment where a key is generated by a PLD each time the PLD is powered on and stored in flip-flops configured as a shift register, which is a volatile storage. Therefore, Erickson does not teach a key being non-volatile as recited by Applicants. Furthermore, Erickson does not teach maintaining both a device identifier and a private key. In fact, nowhere in Erickson is a device identifier even suggested. The embodiments of Erickson only contemplate a single key, and no other identifiers or keys are necessary for the methods described in Erickson. Therefore, Erickson does not teach a non-volatile device identifier and private key maintained in a programmable logic device as claimed by Applicants.

In addition, Erickson does not teach receiving an encrypted key onto the programmable logic device. As noted above, PLD 110 generates a key 180 that is communicated to storage device 120.

That is, the key is transmitted by the PLD and received by the storage device in Erickson, and nowhere in Erickson is it even suggested that PLD 110 receives any kind of key, much less an encrypted key. In fact, Erickson specifically notes that it is important that PLD 110 generate a new key each time it is powered up to enhance security. (See Erickson at col. 3, lines 42-51.) Thus, the act of generating a key is necessary for Erickson, and Applicants submit it would not have been obvious for one of ordinary skill in the art to remove the necessary random number generator from Erickson's PLD in the manner suggested by the Examiner.

Therefore, for at least these reasons, Applicants believe Claim 1 is allowable over the cited art, and respectfully request allowance of Claim 1.

Dependent Claims 2-9 and 11-18

Claims 2-9 and 11-18 depend, either directly or indirectly, from Claim 1, and thus include all of the limitations of Claim 1. Therefore, for at least the reasons set forth above with respect to Claim 1, Applicants believe Claims 2-9 and 11-18 are also allowable, and respectfully request allowance of these claims.

Claims 10, 19 and 29

Claims 10, 19 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Redman et al., U.S. Patent No. 5,978,476 ("Redman") in view of Erickson. Applicants respectfully traverse this rejection.

With respect to Claims 10 and 19, the Examiner stated: "Redman discloses a PLD to realize an IP module (column 2 lines 29-59)," and further stated: "It would have been obvious . . . to configure Redman's PLD with Erickson's encrypted bit stream." (Office Action at page 4, ¶ 7.) Applicants respectfully disagree with the Examiner's allegations. In particular, Applicants submit that Redman does not disclose a PLD to realize an IP module. In fact, the section of Redman cited by the

Examiner does not even mention the terms "PLD" or "IP module" or any related term. Programmable logic devices (PLDs) are only briefly mentioned in the background section of Redman merely as an example of a logic device. Redman, in fact, discloses methods and systems for distributing information to users, without fully revealing the information, for limited evaluation. (See, e.g., Redman at col. 2, lines 29-32.) As noted in Redman, the purpose of Redman's invention is to allow a user to determine whether a function design is suitable for the user's overall design prior to actual purchase by allowing a user to compile the function design using a computer application program. (See, e.g., Redman at col. 1, lines 44-57.) That is, Redman allows a design to be used with certain computer application programs, but does not disclose methods for configuring a PLD. In contrast, the present invention relates to a method and apparatus for securing configuration data used to configure a programmable logic device. Thus, Redman merely discloses a method for pre-purchase trial of a design function, and therefore it would not have been obvious to combine Redman and Erickson in the manner suggested by the Examiner.

Moreover, *prima facie* obviousness has not been established since the Examiner has failed to establish a correspondence between the claimed invention and the teachings of the references. For example, Claim 19 recites "receiving onto a programmable logic device an encrypted first key" and "decrypting the encrypted first key to generate a first key." Neither Redman nor Erickson disclose or even suggest at least these limitations. As noted above, Redman merely mentions PLDs in passing in the background, and does not disclose or suggest a PLD receiving any kind of key, much less an encrypted key that is later decrypted. Erickson also fails to teach or disclose such a steps. As detailed above, Erickson discloses that a key must be generated by the PLD and then sent to a storage device. That is, as shown in Fig. 1 of Erickson, a key 180 is passed from the PLD 110 to the storage device 120. Since the key originates in the PLD, no key is received by the PLD. Thus,

neither Redman nor Erickson teach or even suggest that a PLD receives an encrypted key, as recited by Applicants. Further, just as in Redman, Erickson does not teach that key 180 is encrypted. Thus, it would be impossible for Redman or Erickson, alone or in any combination, to teach the step of decrypting the encrypted first key.

For at least these reasons, Applicants believe Claim 19 is allowable, and respectfully request allowance of Claim 19.

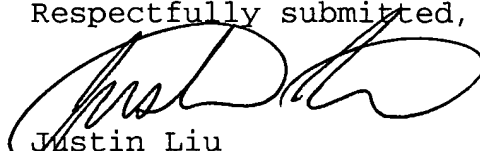
In addition, Claim 10 depends from Claim 1, and thus includes all of the limitations of Claim 1. Therefore, for at least the reasons set forth above with respect to Claim 1, Applicants believe Claim 10 is also allowable, and respectfully request allowance of Claim 10.

Claim 29 depends from Claim 19, and thus includes all of the limitations of Claim 19. Therefore, for at least the reasons presented above with respect to Claim 19, Applicants believe Claim 29 is also allowable, and respectfully request allowance of Claim 29.

Conclusion

In light of the above remarks, Applicants believe that Claims 1-29 are in condition for allowance, and allowance of the application is therefore respectfully requested. If action other than allowance is contemplated by the Examiner, the Examiner is respectfully requested to telephone Applicants' attorney, Justin Liu, at 408-879-4641.

Respectfully submitted,



Justin Liu
Attorney for Applicants
Reg. No. 51,959

I hereby certify that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450, on June 8, 2004.

Julie Matthews
Name



Signature